UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,759	02/18/2004	Markus Miettinen	39700-612001US/NC43225US	9776

64046 7590 12/01/2009

MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C
ONE FINANCIAL CENTER
BOSTON, MA 02111

EXAMINER	
KIM, PAUL	

ART UNIT	PAPER NUMBER
2169	

MAIL DATE	DELIVERY MODE
12/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,759	MIETTINEN ET AL.	
	Examiner	Art Unit	
	PAUL KIM	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-9,12-18,21-25,28-34,37-40,43 and 44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-9,12-18,21-25,28-34,37-40,43 and 44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the following communication: Request for Continued Examination filed on 13 November 2009.

2. Claims 1-2, 5-9, 12-18, 21-25, 28-34, 37-40, and 43-44 are pending and present for examination. Claims 1, 8, 15, 17, 24, 31, 33, and 39 are in independent form.

Response to Amendment

3. Claims 1, 8, 15, 17, 24, 31, 33, and 39 have been amended.

4. No claims have been newly added.

5. No claims have been further cancelled.

Specification

6. Applicant's Amendment to claims 17-30 have been acknowledged. Accordingly, the objection to the Specification is withdrawn.

Claim Rejections - 35 USC § 101

7. Applicant's Amendment to claims 17-30 have been acknowledged. Accordingly, the rejections under 35 U.S.C. 101 are withdrawn.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 1, 2, 5, 6, 8, 9, 12, 13, 15-19, 24, 25, 28, 29, 31-34, 37, 39, 40, 42, and 43** are rejected under 35 U.S.C. 103(a) as being unpatentable over Owen et al (U.S. Patent No. 6,968,349, hereinafter referred to as OWEN), filed on 16 May 2002, published on 20 November 2003, and issued on 22 November 2005, in view of Pond et al (U.S. Patent No. 4,864,616, hereinafter referred to as POND), filed on 15 October 1987, and issued on 5 September 5, 1989, and in further view of Brown et al (USPGPUB 2003/0023850, hereinafter referred to as BROWN), filed on 26 July 2001, and published on 30 January 2003.

10. **As per independent claims 1 and 17,** OWEN, in combination with POND and BROWN, discloses:

A method, comprising:

receiving a second data record to be stored on a single database, wherein the database comprises a first data record {See OWEN, C8:L6-24, wherein this reads over "the minimized data journal entry is read"};

storing the second data record on the database, wherein the second data record is stored consecutive to the first data record {See OWEN, C8:L38-54, wherein this reads over "the validation value comprises a checksum that is computed using both the data in the old record and the metadata for the old record"};

retrieving a first integrity checksum stored with the first data record previous to the second data record {See OWEN, C8:L38-54, wherein this reads over "the validation value comprises a checksum that is computed using both the data in the old record and the metadata for the old record"; and C8:L55-C9:L10, wherein this reads over "[t]he validation value of the preferred embodiments is a value that relates to the state of the record that corresponds to the journal entry just before applying the changes reflected in the journal entry"};

computing a second integrity checksum for the second data record with a cryptographic method using a storage key, the retrieved first integrity checksum and the second data record {See OWEN, C10:L8-27, wherein this reads over "[w]hen the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first computed using the same algorithm used to compute the validation value stored in the journal entry"}, wherein the storage key represents an identity of a signing entity authorized to sign data records {See BROWN, Para. 0049, wherein this reads over "[t]he private key further encrypts a checksum determined for the contents log file that is stored with the signature"};

storing the second integrity checksum on the database {See OWEN, C10:L8-27, wherein this reads over "[t]his validation value is then stored as apart of the minimized data journal entry"}; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector {See POND, C3:L53-62, wherein this reads over "[t]he initialization vector contains bits for indicating the starting bye in each of the key streams used for

> encryption and decryption. The Checksum is derived by summing the . . . the Initialization Vector and issued to confirm the integrity of the label"} or a digital signature of a signing entity.

While OWEN may fail to expressly disclose a method for configuring a retrieved integrity checksum for a first row of the database to be a generated initialization vector, POND discloses a method wherein an initialization vector is used to derive a checksum. The combination of inventions disclosed in OWEN and POND would disclose a method wherein the integrity checksum for a first row of a database is a generated initialization vector. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by POND.

One of ordinary skill in the art would have been motivated to do this modification so that where there is no previous integrity checksum available, the initialization vector may be used to in the computation of a second integrity checksum.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a private key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

11. **As per dependent claims 2, 18, and 34,** OWEN, in combination with POND and BROWN, discloses:

The method according to claim 8, further comprising:

> configuring the storage key to be a secret key of public key infrastructure {See BROWN, Para. 0049, wherein this reads over "[t]he private key further encrypts a checksum determined for the contents log file that is stored with the signature"}.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a private key used for verification purposes in a public key infrastructure. Therefore, it

would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

12. **As per dependent claims 5, 12, 21, 28, 37, and 43,** OWEN, in combination with POND and BROWN, discloses:

> The method according to claim 8, wherein the retrieving the first integrity checksum comprises retrieving the first integrity checksum from a memory of a verification entity {See OWEN, C8:L8-24, wherein this reads over "[t]he generated validation value is then compared against the validation value stored in the minimized data journal entry"}.

13. **As per dependent claims 6, 13, 22, and 29,** OWEN, in combination with POND and BROWN, discloses:

> The method according to claim 8, further comprising:
>
> storing the second integrity checksum on a memory of a verification entity {See OWEN, C10:L8-27, wherein this reads over "[t]his validation value is then stored as apart of the minimized data journal entry"}.

14. **As per independent claims 8, 15, 24, 31, 33, and 39,** OWEN, in combination with POND and BROWN, discloses:

> A method, comprising:
>
> retrieving a second data record to be verified from a single database {See OWEN, C8:L6-24, wherein this reads over "the minimized data journal entry is read"};
>
> retrieving a second integrity checksum of the second data record, wherein the first data record and the second data record are consecutive data records in the database {See OWEN, C8:L38-54, wherein this reads over "[a]nother type of suitable validation value is a cyclic redundancy check (CRC) that provides a unique value that indicates the state of the record before applying the change"; and C10:L8-27, wherein this reads over "[w]hen the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first computed using the same algorithm used to compute the validation value stored in the journal entry"};
>
> retrieving a first integrity checksum of the first data record previous to the retrieved second data record {See OWEN, C8:L38-54, wherein this reads over "the validation value comprises a checksum that is computed using both the data in the old record and the metadata for the old record"; and C8:L55-C9:L10, wherein this reads over "[t]he validation value of the preferred embodiments is a value that relates to the state of the record that corresponds to the journal entry just before applying the changes reflected in the journal entry"};

computing a third integrity checksum for the second data record using the retrieved second data record, the first integrity checksum, and a storage key {See OWEN, C10:L8-27, wherein this reads over "[w]hen the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first computed using the same algorithm used to compute the validation value stored in the journal entry"}, wherein the storage key represents an identity of a signing entity authorized to sign data records {See BROWN, Para. 0049, wherein this reads over "[t]he private key further encrypts a checksum determined for the contents log file that is stored with the signature"}; and

comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal {See OWEN, C10:L8-27, wherein this reads over "[i]f the two validation values match, we know with a high level of confidence that the record is in the identical state it was in just before the changes reflected in the journal entry were made"}; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector {See POND, C3:L53-62, wherein this reads over "[t]he initialization vector contains bits for indicating the starting bye in each of the key streams used for encryption and decryption. The Checksum is derived by summing the . . . the Initialization Vector and issued to confirm the integrity of the label"} or a digital signature of a signing entity.

While OWEN may fail to expressly disclose a method for configuring a retrieved integrity checksum for a first row of the database to be a generated initialization vector, POND discloses a method wherein an initialization vector is used to derive a checksum. The combination of inventions disclosed in OWEN and POND would disclose a method wherein the integrity checksum for a first row of a database is a generated initialization vector. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by POND.

One of ordinary skill in the art would have been motivated to do this modification so that where there is no previous integrity checksum available, the initialization vector may be used to in the computation of a second integrity checksum.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a private key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

15. **As per dependent claims 9, 25, and 40,** OWEN, in combination with POND and BROWN, discloses:

The method according to claim 8, further comprising:

configuring the storage key to be a public key of public key infrastructure {See BROWN, Para. 0061, wherein this reads over "In particular, to verify the participants in a messaging session, logging controller 62 utilizes a public key for a user to attempt to decrypt the private key and checksum. If a private key matches a public key, then an identity for a user associated with the public and private keys may be verified. Further, logging controller 62 utilizes the public key to decrypt a checksum for the recorded messaging session and then computes a current checksum for the messaging session. If the checksums match, then the integrity of the messaging session may be verified. In addition, methods other than calculating a checksum may be utilized to verify the integrity of the messaging session"}.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a public key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

16. **As per dependent claims 16 and 32,** OWEN, in combination with POND and BROWN, discloses:

The system according to claim 15, wherein the signing entity and verification entity apply public key infrastructure {See BROWN, Para. 0061, wherein this reads over "In particular, to verify the participants in a messaging session, logging controller 62 utilizes a public key for a user to attempt to decrypt the private key and checksum. If a private key matches a public key, then an identity for a user associated with the public and private keys may be verified. Further, logging controller 62 utilizes the public key to decrypt a checksum for the recorded messaging session and then computes a current checksum for the messaging session. If the checksums match, then the integrity of the messaging session may be verified. In addition, methods other than calculating a checksum may be utilized to verify the integrity of the messaging session"} for calculating and verifying the one of the first integrity checksum and the second integrity checksum .

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a public key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

17. **Claims 7, 14, 23, 30, 38, and 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over OWEN, in view of POND, and in further view of Cain (U.S. Patent No. 6,557,044, hereinafter referred to as CAIN), filed on 1 June 1999, and issued on 29 April 2003.

18. **As per dependent claims 7, 14, 23, 30, 38, and 44,** OWEN, in combination with POND and CAIN discloses:

The method according to claim 8, further comprising:

configuring the integrity checksums to comprise a running sequence number {See CAIN, c2:l64-67, wherein this reads over "incremental checksumming may be utilized. Initially, the checksum for all routes in a set is computed by determining the checksum for all sequence numbers"}.

Response to Arguments

19. Applicant's arguments filed 13 November 2009 have been fully considered but they are not persuasive.

a. Claim Rejections under 35 U.S.C. 103

Applicant asserts the argument that "Owen is completely silent with respect to an integrity checksum computed using a storage key and the second data record, where the second data record is to be stored on a single database." See Amendment, page 13. The Examiner respectfully disagrees. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the second data record is to be stored in a single database) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). It is noted that claim 1 recites a method wherein the second data record is stored on the database and then subsequently the second integrity checksum is computed.

With regards to the newly added claim limitation, Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Accordingly, the rejections under 35 U.S.C. 103 are sustained.

Conclusion

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PAUL KIM whose telephone number is (571)272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tony Mahmoudi can be reached on (571) 272-4078. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tony Mahmoudi/
Supervisory Patent Examiner, Art Unit 2169

Paul Kim
Examiner, Art Unit 2169
TECH Center 2100

/pk/